USER-TRUST-DRIVEN VIDEO ORGANIZATION IN SOCIAL MEDIA

[1] *Mr. A. Sandeep,* [2] *P.Shashank,* [3] K.Koushik Reddy, [4] *P.Rahul Reddy,*[5] *P.Niranjan Reddy*
[1] Assistant *Professor,*[2345]*B.Tech Students*
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

Social Multimedia Networks (SMNs) have attracted much attention from both academia and industry due to their impact on our daily lives. The requirements of SMN users are increasing along with time, which make the satisfaction of those requirements a very challenging process. One important challenge facing SMNs consists of their internal users that can upload and manipulate insecure, untrusted and unauthorized contents. For this purpose, controlling and verifying content delivered to end-users is becoming a highly challenging process. So far, many researchers have investigated the possibilities of implementing a trustworthy SMN. In this vein, the aim of this paper is to propose a framework that allows collaboration between humans and machines to ensure secure delivery of trusted videos content over SMNs while ensuring an optimal deployment cost in the form of CPU, RAM, and storage. The key concepts beneath the proposed framework consist in i) assigning to each user a level of trust based on his/her history,

ii) creating an intelligent agent that decides which content can be automatically published on the network and which content should be reviewed or rejected, and iii) checking the videos' integrity and delivery during the streaming process. Accordingly, we ensure that the trust level of the SMNs increases. Simultaneously, efficient Capital Expenditure (CAPEX) and Operational Expenditures (OPEX) can be achieve.

I. INTRODUCTION

The recent advances in the Internet have resulted in the emergence of many web applications and social multimedia networks (SMN). These applications (e.g., Facebook, Twitter, and Google) have revolutionized the use of the Internet as a tool to interconnect people over the world. The features implemented by these service providers have been making communication between people easier. Service providers have granted to the users more flexibility for interacting among themselves and exchanging different social information. Thanks to these services, users can easily discuss their ideas and opinions remotely, publish new articles, and meet new persons. Moreover, they have allowed business and organizations to advertise for their products over the world and to directly contact their customers. In addition to these social networks, other web applications, such as YouTube, Dailymotion, and Vimeo, have enabled the exchange of different contents, including text, images, and videos among different entities connected to their services. The evolution of the Internet and distributed systems has led researchers to implement applications that serve video on demand (VOD) on top of the peer- to-peer (P2P) networks. VOD and videos live streaming systems are gaining momentum in SMN. They have enabled the appearance of many multimedia-centric services such as video conferencing applications, online meeting applications, massive open online courses (MOOC) as well as other use cases in e-health and e-teaching. Such services attract and connect millions of users worldwide. The providers of these services have enabled countless features that allow users to interact among themselves by creating and sharing different contents (e.g., videos, text, and images). However, by allowing this, the nodes composing the social networks, users and machines, generate a huge amount of data, which can be uncontrolled, unsecured and untrusted; Such amount of generated data is causing a congestion to the networks, and posing a new security challenge to the service providers: it becomes hard to handle and analyze all content traversing their networks. Additionally, the trust score provides decisional systems with the needed information to execute adequate actions, such as the implementation of certain policies that restraint an entity from using some resources or accessing some services.

The main features that should be taken into consideration while defining a trust model are as follows:

- User history: The only way to predict user behavior is to study and analyze all generated content by different users during their interactions in the network. The user history records may contain relations and links between data, these links are valuable for the data analytics applications in order to offer a good user experience.
- Trust calculation: A user's level of trust is one of the important metrics that should be taken into consideration when analyzing users' data. The computation of this value includes the selection of various parameters that characterize the manipulated data. For this reason, there is a need to suggest a realistic model that can capture the characteristics of uploaded data based on the historical behavior of users.
- Users collaboration: Based on the observation that human intelligence is one of the main keys to effectively detect and remove untrusted data, many algorithms and applications have been recently devised for detecting and measuring users' collaborations rate. These algorithms and applications allow users to rate different social multimedia items. Then, the system is able to collect these feedbacks, applies some filtering methods and executes different needed actions.

Secure content delivery: In a trustworthy social network, every bit of data should be under control. In other words, starting from any node in the network (e.g, user, mobile, or server), the path that the data take to arrive at another node should be secured. Besides the user trust calculation module, the generic framework has: i) a voting service to allow users rewarding trusted clients and penalizing malicious users; ii) an incentive module to remunerate the users for their collaboration; iii) secure videos module that ensures secure delivery of videos; and iv) a video integrity checker service to assure the integrity and timestamping of uploaded videos. Moreover, an adaptation on the video player, at the client side, is also proposed to take into consideration the new features suggested in the new framework. The update consists of implementing a new functionality at the video player that enables it to communicate with the video integrity checker and verify that the chunks buffered were not altered during the streaming process. Furthermore, the proposed generic framework has a video uploading decision process module that enables checking the quality of the uploaded videos before either accepting the publication or not. Besides the use of historical behavior of users, this module explores two techniques for checking the quality of the uploaded contents: i) analytical checking of the uploaded videos; ii) review checking of the uploaded contents by a set of trusted users.

II. LITERATURE SURVEY

1. A popularity driven video discovery scheme for the centralized p2p-vod system

With the popularity of network, P2P-based Video on Demand (VoD) has become one of the main services in Internet. However, due to the huge number of videos, how to access the video quickly is important since it affects the subscriber's experience. In this paper, a popularity-driven storing model is proposed to fasten the video discovery for a centralized P2P-VoD system. All videos are stored in a binary tree in the server according to their popularities. Experimental results show that this scheme works well in terms of discovery delay and resource utilization.

2. Toward trustworthy social network services: A robust design of recommender systems.

In recent years, electronic commerce and online social networks (OSNs) have experienced fast growth, and as a result, recommendation systems (RSs) have become extremely common. Accuracy and robustness are important performance indexes that characterize customized information or suggestions provided by RSs. However, nefarious users may be present, and they can distort information within the RSs by creating fake identities (Sybils). Although prior research has attempted to mitigate the negative impact of Sybils, the presence of these fake identities remains an unsolved problem. In this paper, we introduce a new weighted link analysis and influence level for RSs resistant to Sybil attacks. Our approach is validated through simulations of a broad range of attacks, and it is found to outperform other state-of-the-art recommendation methods in terms of both accuracy and robustness.

3. Coping with emerging mobile social media applications through dynamic service function chaining

User generated content (UGC)-based applications are gaining lots of popularity among the community of mobile internet users. They are populating video platforms and are shared through different online social services, giving rise to the so-called mobile social media applications. These applications are characterized by communication sessions that frequently and dynamically update content, shared with a potential number of mobile users, sharing the same location or being dispersed over a wide geographical area. Since most of UGC content of mobile social media applications are exchanged through mobile devices, it is expected that along with online social applications, this content will cause severe congestion to mobile networks, impacting both their core and radio access networks. In this paper, we address the challenges introduced by these applications devising a complete framework that 1) identifies such applications/sessions and 2) initiates multicast-based delivery (or offload through Wi-Fi) of the relevant content. The proposed framework leverages the network function virtualization (NFV) paradigm to dynamically integrate its functionalities to the operators' service function chaining (SFC) process, allowing fast deployment and lowering both capital and operational expenditures (CAPEX and OPEX) of the mobile operators. The performance of the proposed framework is evaluated through mathematical analysis and computer simulations, taking Twitter-like social applications as an example.

4. Impact of emerging social media applications on mobile networks

Emerging social media applications are expected to cause severe congestion to mobile networks, both mobile core network and mobile radio access network. These social media applications are characterized by the fact that they involve sessions with frequently and dynamically updated content, shared with a potential number of mobile users sharing the same location, or being dispersed over a wide area. A method to dynamically identify such applications/sessions and initiate multicast-based delivery of the relevant content is proposed. The performance of the proposed method is evaluated through computer simulations, taking Twitter as an example. Encouraging results are obtained.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

Ensuring a secure delivery of trusted videos and preventing users of social networks from manipulating insecure, untrusted and unauthorized contents is a challenging process that needs a high amount of computational power. Most research work, published concerning the trustworthiness among entities in a network, have studied the trust level in a way that they compute the degree of trust amongst users in SMN.

DISADVANTAGES OF EXISTING SYSTEM:

There is no automatic way to prevent users from uploading insecure, untrusted and unauthorized contents

PROPOSED SYSTEM:

The main goal of the generic framework is to create a system that is able to provide secure delivery of trusted videos content over social networks with low resources consumption in terms of CPU, RAM, and storage The proposed framework explores both the user history and users' collaboration for taking the decision to either make the analytical analysis or not. The framework contains a module that is responsible for calculating the level of trust of each user in the network

ADVANTAGES OF PROPOSED SYSTEM:

The proposed system reduces the resource utilization

Reduces the cost, by analyzing only the video shared by social multimedia network.

SYSTEM ARCHITECTURE

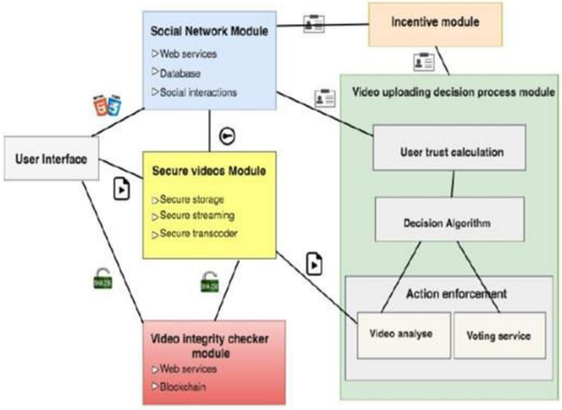


Fig: System Architecture

IV. IMPLEMENTAIONS

MODULES

- SOCIAL NETWORK MODULE
- SECURE VIDEOS MODULE
- VIDEO INTEGRITY CHECKER MODULE
- INCENTIVE MODULE
- TRUST CALCULATION MODULE
- VOTING SYSTEM MODULE

MODULE DESCRIPTION ADMIN

SOCIAL NETWORK MODULE(SNM)

This module is the first component that interacts with the users. It permits them to do all kind of social interactions, such as the upload of videos, the post of comments, and the sharing of different videos. This module is composed of many microservices that communicate with each other in order to offer a user-friendly application that fulfills the end-users needs. The main micro-services are

i. the web server that responds to the users' requests,

ii. a database that stores all information of users and their generated content,

iii. a caching microservice for reducing the response time and allowing the users to have good experiences while interacting with the system,

iv. a message broker that allows the communication between the different components, and

v. a central authentication service that authenticates the users and gives them the right to request other services.

SECURE VIDEOS MODULE(SVM)

This module allows authorized users to upload their media files to the secure storage, as well as it allows the social network users to watch the videos streamed on demand from the secure streaming. The SVM consists of three components:

Secure storage: this component mainly works as follows: first of all, an authorized user sends an upload request to the SNM. Then, the social network module (SNM), more precisely the central authentication micro-service, generates and stores a unique token in the database, and then sends it to the user as a response. The user starts sending the video chunks to the storage server while including that token within the messages sent. The storage server (SS) checks the received token and then decides either to accept or reject the upload. This component adopts the HTTP live stream (HLS) for serving diverse users with different resolutions adapted to their network bandwidth and devices. Also, this component uses the Rivest Cipher 4 (RC4) algorithm in order to encrypt the video chunks sent to the end users.

Secure transcoder: this component allows the transcoding of the uploaded videos to different resolutions using software's such as FFMPEG. Each resolution is subdivided into small chunks of fixed time duration [35]. After the transcoding operation ends, the secure transcoder creates a hash for each chunk and sends that hash to the video integrity checker module (VICM). The VICM saves that hash in a public or private BLOCKCHAIN service as a transaction. The hashed values will be used by the user video player to verify that the chunks received were approved by the system and the chunks were not modified from the time that a user uploaded the video to the secure storage.

VIDEO INTEGRITY CHECKER MODULE (VICM)

The main feature of this module is to allow the timestamping of the chunks generated from an uploaded video. This helps in checking the integrity of these chunks in the future. Formally, the VICM module saves the video content, its signature and its date-time of creation in a trusted and a shared database. Also, this module checks that the file has not been altered or modified thanks to Blockchain technologies. Moreover, the service will be also used from a client (e.g, browser, tablet, smartphone, etc) to verify that the video chunks received were not altered during the streaming process.

INCENTIVE MODULE (IM)

In order to motivate users to review some uploaded videos and decide to publish them or not, an incentive component was created to reward the users for their contributions. This component is responsible for remunerating the reviewers when they make a true vote. A vote is considered true when the decision made at the proposed framework is to publish the uploaded video.

TRUST CALCULATION MODULE

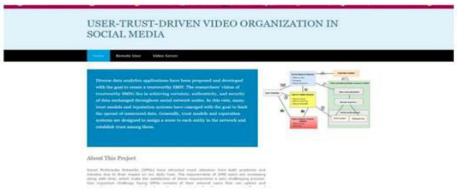
This sub-module has the responsibility to compute the trustworthiness of different users. For this reason, it keeps monitoring the behavior of each user by taking into consideration his/her social interactions with other users. These social interactions include, but not limited to, the following parameters: i) the number of followers (NOF); ii) the number of true votes (NOTV) received from trusted users through the voting service sub-module; iii) the percentage of true reports (PTR) received from different users of the social network; iv) the percentage of likes (POL) received from the user network mainly his friends; and v) the average trust of published videos (ATPV). For the sake of simplicity, the trust value of each user is computed using a weighted sum function of the different parameters. However, any more sophisticated method can be also used with slight modification. For instance, the entropy of Shannon can be also applied to these parameters for computing the trust degree of each user. In what follows, we will show how the trust values of users and videos are computed.

VOTING SYSTEM MODULE

The voting service is one of the main components of the system. It allows users to review and vote certain videos in order to be published or not. It also permits users to reestablish their trust level. The set of reviewers is selected according to a method that ensures that there is always a sufficient number of reviewers. The method also allows a subset of users with low values of trust to re-establish their reputations and gradually increase their factor of trust. Moreover, the voting service collects votes and sends the gathered data to the decision-making algorithm. The decision algorithm explores the received feedbacks to take decisions on whether to publish or not a video.

V. SCREENSHOTS

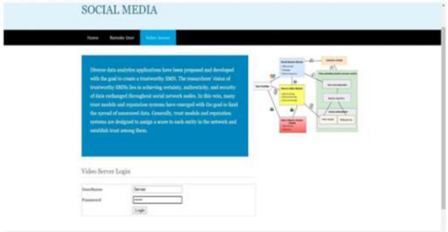
A home page is a webpage that serves as the starting point of website. It is the default webpage that loads when you visit a web address that only contains a domain name



Diverse data analytics applications have been proposed and developed with the goal to create a trustworthy SMN. The researchers' vision of trustworthy SMNs lies in achieving certainty, authenticity, and security of data exchanged throughout social network nodes. In this vein, many trust models and reputation systems have emerged with the goal to limit the spread of unsecured data. Generally, trust models and reputation systems are designed to assign a score to each entity in the network and establish trust among them.

About This Project

FIG 2: VIDEO SERVER LOGIN

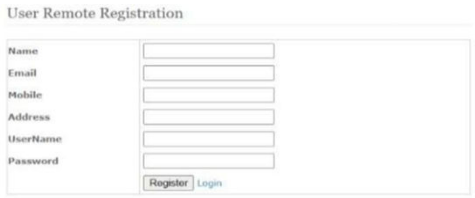


Diverse data analytics applications have been proposed and developed with the goal to create a trustworthy SMN. The researchers' vision of trustworthy SMNs lies in achieving certainty, authenticity, and security of data exchanged throughout social network nodes. In this vein, many trust models and reputation systems have emerged with the goal to limit the spread of unsecured data. Generally, trust models and reputation systems are designed to assign a score to each entity in the network and establish trust among them.

Video Server Login

UserName	Server
Password	•••••

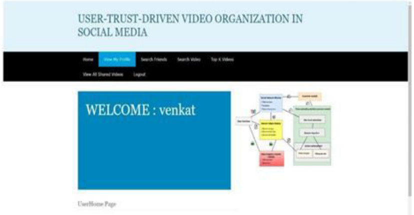
FIG 3 : USER REGISTRATION PAGE



User Remote Registration

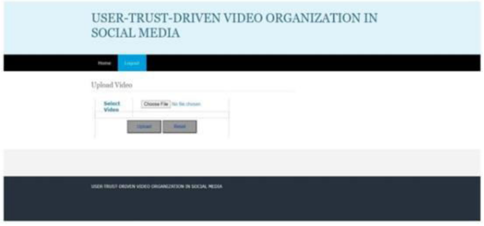
Name	
Email	
Mobile	
Address	
UserName	
Password	

FIG 4 : USER DETAILS



WELCOME : venkat

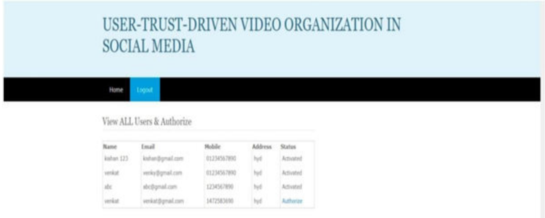
FIG 5: UPLOAD VIDEO


USER-TRUST-DRIVEN VIDEO ORGANIZATION IN SOCIAL MEDIA
Home
Logout
Choose File
No file chosen
Upload
Reset
USER-TRUST-DRIVEN VIDEO ORGANIZATION IN SOCIAL MEDIA

Upload Video

Select Video

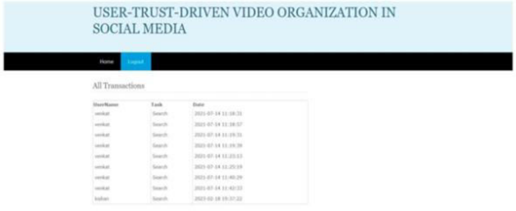
FIG 6: VIEW USERS AND AUTHORIZE



View ALL Users & Authorize

Name	Email	Mobile	Address	Status
kishan 123	kishan@gmail.com	01234567890	hyd	Activated
venkat	venky@gmail.com	01234567890	hyd	Activated
abc	abc@gmail.com	1234567890	hyd	Activated
venkat	venkat@gmail.com	1472583690	hyd	Authorize

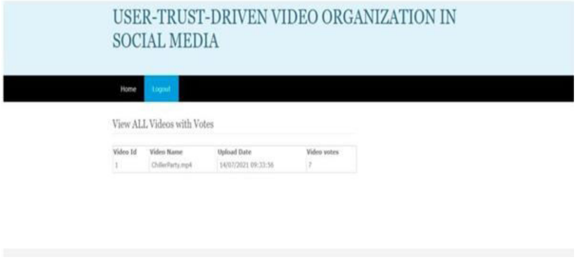
FIG 7: USER TRANSACTION



All Transactions

UserName	Task	Date
venkat	Search	2021-07-14 11:18:21
venkat	Search	2021-07-14 11:18:57
venkat	Search	2021-07-14 11:19:31
venkat	Search	2021-07-14 11:19:39
venkat	Search	2021-07-14 11:23:13
venkat	Search	2021-07-14 11:25:19
venkat	Search	2021-07-14 11:40:29
venkat	Search	2021-07-14 11:42:22
kishan	Search	2023-02-18 19:37:22

FIG 8: ALL VIDEOS AND THEIR VOTES



USER-TRUST-DRIVEN VIDEO ORGANIZATION IN SOCIAL MEDIA

View ALL Videos with Votes

Video Id	Video Name	Upload Date	Video votes
1	ChillerParty.mp4	14/07/2021 09:33:56	7

VI. CONCLUSION

CONCLUSION

Their services are becoming the most popular ones among the community of Internet users. The data generated and exchanged by users of these networks become diverse. They include videos, documents, text, and pictures. Unfortunately, there are users that can insert insecure, untrusted and unauthorized contents. Thus, there is need for an effective way to control and verify the exchanged content. In this work, we focused on how to ensure that the users upload only secured, trusted and authorized videos to the social multimedia networks. We therefore proposed a complete framework that takes into account different aspects to attribute trust values to both users and content and to accordingly secure video streaming. The proposed framework has been designed in a way to reduce the resources utilization in terms of CPU, RAM, and storage. Moreover, we proposed a video uploading decision process module that leverages the historical behaviors of users for making the right decisions on either allowing or denying the upload of videos. This module uses an infinite discrete Markov decision process (DMDP) for taking those decisions. Also, this module can decide for either to analytically check the contents or send them to external reviewers before publishing them or forbidding their publication. The simulation results demonstrate the efficiency of the proposed algorithm in terms of publishing the good contents and forbidding the bad ones. Also, the simulation results demonstrate the efficiency of proposed algorithms in terms of minimizing the incurred computational cost.

FUTURE SCOPE

The future scope of user trust-driven video organization in social media could involve several advancements and enhancements to improve user experience, safety, and engagement. Here are some potential future developments in this area:

1. **Advanced Trust Algorithms:**
Develop more sophisticated algorithms for assessing and calculating user trust. This could include machine learning and artificial intelligence techniques to analyze user behavior, content interactions, and community feedback to generate more accurate trust scores.

2. **Enhanced Content Moderation:**
Implement advanced content moderation tools that use AI and natural language processing to detect and filter out inappropriate or harmful content. This could help create a safer and more positive environment for users.

3. **Blockchain for Trust and Transparency:**
Explore the use of blockchain technology to enhance trust and transparency in social media platforms. Blockchain can provide a decentralized and tamper-proof record of interactions, building a more trustworthy system for users.

4. **Decentralized Social Media Platforms:**
Develop decentralized social media platforms that give users more control over their data and interactions. This could address concerns related to centralized authority and privacy issues.

REFERENCES

1. L. Gao, H. Ling, X. Fan, J. Chen, Q. Yin, and L. Wang, “A popularity-driven video discovery scheme for the centralized p2p-vod system,” in 2016 8th International Conference on Wireless Communications Signal Processing (WCSP), Oct 2016, pp. 1–4.
2. W. Chang and J. Wu, “Social vod: A social feature-based p2p system,” in 2015 44th International Conference on Parallel Processing, Sept 2015, pp. 570–579.
3. T. Taleb, N. Kato, and Y. Nemoto, “Neighbors-buffering-based video on-demand architecture,” Signal Processing: Image Communication, vol. 18, no. 7, pp. 515 – 526, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0923596503000390
4. T. Taleb and N. Taleb, “System and method for creating multimedia content channel customized for social network.” Patent PCT/US2011/049 159, Nov, 2011.
5. Statista. Social media usage worldwide.

[Online]. Available: https://www.statista.com/study/12393/social networks-statista-dossier/

6. G. Noh, H. Oh, K. h. Lee, and C. k. Kim, "Toward trustworthy social network services: A robust design of recommender systems," Journal of Communications and Networks, vol. 17, no. 2, pp. 145–156, April 2015.
7. T. Taleb, A. Ksentini, M. Chen, and R. Jantti, "Coping with emerging mobile social media applications through dynamic service function chaining," IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2859–2871, April 2016.
8. T. Taleb and A. Ksentini, "Impact of emerging social media applications on mobile networks," in 2013 IEEE International Conference on Communications (ICC), June 2013, pp. 5934–5938.
9. L. Yang, Z. Zhang, W. Tian, and Q. Chen, "Advance on trust model and evaluation method in social networks," in 2012 Sixth International Conference on Genetic and Evolutionary Computing, Aug 2012, pp. 9–14.
10. X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 310–320, Feb 2014.
11. M. K. Rahman and M. A. Adnan, "Dynamic weight on static trust for trustworthy social media networks," in 2016 14th Annual Conference on Privacy, Security and Trust (PST), Dec 2016, pp. 62–69.
12. S. Hussain, N. Honeth, R. Gustavsson, C. Sandels, and A. Saleem, "Trustworthy injection/curtailment of der in-distribution network maintaining quality of service," in 2011 16th International Conference on Intelligent System Applications to Power Systems, Sept 2011, pp. 1–6.
13. A. Ganz and A. Kumar, "A systems approach to teaching trustworthy computing," in 2007 37th Annual Frontiers In Education Conference - Global Engineering: Knowledge Without Borders, Opportunities Without Passports, Oct 2007, pp. S1C–15–S1C–18.